SUBJECT ACCESS REQUEST POLICY

MAY 2019

CONTENTS

Introduction

Oasis is committed to honest and open relationships as part of the work we undertake in transforming communities as a fundamental part of our ethos. As part of this commitment, we openly and willingly share the information we process about individuals with them to the extent that is possible, and where we are able to do so under the applicable regulations and legislation.

Subject Access Requests ("SARs") are the legal mechanism under which individuals can request access to the personal data that we process about them, and they serve a valuable purpose in reassuring data subjects that data held about them is accurate and has been fairly and lawfully processed.

a. Purpose

The purpose of this document is to set out how Oasis will handle Subject Access Requests ("SARs").

It sets out the requirements, responsibilities and accountabilities associated with this policy. Failure to adhere to this policy may lead to disciplinary action being taken. Breaches of this policy may be considered misconduct up to and including gross misconduct.

From time to time, we may amend this policy, so please check back when you next visit this site. Requests to change the policy should be made to the Director of Information Technology.

The objective of this policy is to define how Oasis will manage a Subject Access Request.

b. Policy Scope

This policy applies to the following Oasis Entities:

- Oasis Community Learning (OCL)
  - The Oasis Community Learning National Office
  - All Oasis Community Learning Academies
  - All Oasis Community Learning National Services

- Oasis Community Partnerships (OCP)
  - The Oasis Community Partnerships National Office
  - All Oasis Community Partnerships Hub Charities

- Oasis IT Services Ltd
- The Oasis Charitable Trust
- The Oasis Foundation

c. Related Oasis Policies, Standards and Processes

This policy should be read in conjunction with the following policies:

- The Oasis Data Protection Policy
- The Oasis Confidentiality Policy
- The Oasis Use of Email Policy

This policy should be read in conjunction with the following Oasis IT Services Standards

- The Oasis Device Event Log Configuration Standard

- The Oasis Server Event Log Configuration Standard

This policy should be read in conjunction with the following Oasis IT Services Processes

- The Oasis Subject Access Request Process
- The Oasis IT User Deletion Process
- The Oasis IT User Creation Process

d. Applicable Legislation, Guidance and References

The policy is created with reference to the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR)

e. Changes to this policy

This policy will be reviewed every year, or when significant changes occur in related legislation or in our strategy. When this happens, we will place an updated version on this document and the date the document has been amended will be visible at the bottom of this page.

Definitions

This section includes the definitions of terms used within this document. A full glossary IT Policy Terms is available as a separate document.

Academy Data: This refers to all data residing within each academy. IT relates to both student and Academy Staff data. It includes data which is stored within the Oasis IT Services IT System.

Confidential Data: Confidential Data is information which is held by Oasis, which does not relate to a living individual but that it may be damaging to Oasis if access was obtained to the data by someone who was not authorised to access it. An example of this would be financial information such as commercial contractual data.

Data: For the purposes of this document, Data is any information processed by Oasis. Oasis classifies data into the four categories: General Data, Confidential Data, Personal Data and Sensitive Data.

Data Controller: The organisation that is responsible for the Data. For the purposes of this policy, Oasis Subsidiary or Legal Body is the Data Controller.

Data Processing: See Processing

Data Subject: Any natural person who is the subject of Personally Identifiable Information held by Oasis.

General Data: Data which Oasis holds that is neither personally identifiable nor sensitive. For example, records of the last time that a building was painted or the count of attendance at an Oasis event.

Nationally Held Data:

This refers to all data that is held within National or Central systems relating to National Staff and National Oasis Operations. This includes data relating to Finance, HR, IT and National Procurement. This also includes all data for Governance, Planning, audits and risk.

Oasis Entity: Oasis Entities are business units that make up the Oasis family in the UK and are either part of Oasis Subsidiaries or subsidiaries in their own right. Oasis Entities include Oasis Academies, Oasis Community Learning National Services, Oasis Community Partnerships Hub Charities. Entities may be separate legal entities or part of a subsidiary that is the Legal Entity.

Personal Data: Data relating to a natural person who can be identified from that information or from that data and other information in possession of Oasis. This includes but is not limited to name, address, telephone number, id number. This also includes expression of opinion about the individual, and of the intentions of Oasis in respect of that individual. Information about IT usage including IP address should be considered as Personal Data. Personal data includes information that the Data Subject has supplied about him or herself. It also includes images of the data subject recorded by an Oasis camera.

Personally Identifiable Information (PII):

Is a general collective term to include either Personal or Sensitive Data.

Processing: Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data, Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data Disclosure or otherwise making available of data.

Relevant Filing System:

Any hard copy paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Personal data can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Requester: The individual making a request for access to personal information by the means of a Subject Access Request. This would normally be the Data Subject themselves. However, the requester can also be a third party who is making the Subject Access Request on behalf of the Data Subject.

SAR Manager: the point of contact for the Requester about a SAR and the person within Oasis tasked with responding to the SAR.

Sensitive Data: Oasis terminology for Special Category Data as defined in the Data Protection Act 2018. It is different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual orientation, criminal convictions. OCL's handling of sensitive data is subject to much stricter conditions of processing.

Third Party: Any individual/organisation other than the data subject, Oasis or its agents.

Policy Statement

1. Receiving a Subject Access Request (SAR)

1.1. Oasis adopts a policy of openness in allowing individuals access to their personal information in accordance with our ethos and the applicable data protection regulations. Oasis are committed to being transparent in our processing of personal and sensitive data.

1.2. Oasis will always endeavour to provide access to personal data that we process about a Data Subject to the Data Subject unless we are unable to do so due to legal restriction, regulation or where the disclosure of the information may have an adverse impact on the rights of another Data Subject.

1.3. A Subject Access Request (SAR) is any request made by an individual to obtain copies of personal or sensitive information that Oasis as a Data Controller may be processing about them.

1.4. Oasis will respond to a SAR received in a wide variety of forms including but not limited to verbal requests, requests in writing, requests made electronically or made through social media.

1.5. Oasis do not require Data Subjects to make SARs in a particular form or format for the SAR to be considered valid.

1.6. A SAR can be made to any member of Oasis Staff. However, queries about rights of access, Subject Access Requests and Data Protection should normally be directed to the Data Protection Officer (DPO).

1.7. The requester is not required to state why they wish to access the information.

1.8. The requester should specify information they wish to access (e.g. specific details of information required, where and by whom information is believed to be held, etc.).

1.9. The Data Subject's rights under a SAR are to their own personal data, not to any specific document in which it is contained. Personal data may be extracted from documents and supplied separately under a SAR.

1.10. The requester should provide as much information as possible to assist Oasis in the location of the data required in responding to the SAR.

2. Management of Subject Access Requests

2.1. Accountability for the management of a SAR lies with the Oasis Entity where the Data Subject is or was based.

2.2. The Oasis Entity will assign a responsible person as the 'SAR Manager' to oversee the SAR and to manage its completion in line with this policy. The SAR Manager is not considered a permanent role; rather it will be assigned to an individual on a SAR-by-SAR basis.

2.3. The SAR Manager assigned must be appropriate to the context of the SAR received:

2.3.1. The SAR Manager must be an individual who can be considered to be impartial in any wider relationship with the data subject.

2.3.2. Where the SAR is received from a member of staff then the SAR Manager must be someone of greater seniority than the data subject themselves.

2.4. The Oasis Entity must inform the Data Protection Officer (DPO) that a SAR has been received and provide the contact details for the SAR Manager.

2.5. The DPO must maintain a register of all SARs along with their status.

2.6. The SAR Manager must keep the DPO informed as to the status and progress of the SAR at all times with regular updates.

2.7. The SAR Manager must manage the SAR in accordance with the Oasis SAR Process.

2.8. The DPO is the primary source of expertise in Data Protection matter including issues relating to SARs. The DPO should be consulted for clarification throughout the process of completing the SAR as required. The SAR Manager must follow the direction of the DPO where a course of action is advised in relation to the SAR.

2.9. A SAR may involve other issues unrelated to data protection. In those cases, the responsible manager must ensure that these other issues are addressed under the appropriate policy.

3. Verifying the identity of the requester

3.1. Oasis will only release information in response to a SAR where the identity of the requester can be positively confirmed.

3.2. The requester must provide sufficient information to allow Oasis to verify their identity in order to be able to ascertain if the SAR is valid and if the requester has the right to the information.

3.3. The SAR Manager must record how the identity of the requester has been verified and include this in his or her reporting to the DPO.

3.4. Where the requester is known to Oasis staff through previous interaction then the SAR Manager can consider this to be sufficient to identify the requester.

3.5. The SAR Manager will seek clarification of the requester's identity where required. Where clarification is required, then documented photographic evidence of identity (e.g. passport, driving licence) should be provided. Exceptionally, if photographic evidence is not available, a birth certificate plus recent utility bill should be provided.

4. Cross Oasis Entity SARs

4.1. Unless specifically otherwise requested, standard IT searches will be conducted within the Oasis Entity where the Data Subject is based.

4.2. Where there is a conversation or thread which includes both members of the home Oasis entity and other parts of the organisation then the data returned from the standard IT search will be passed to the relevant Oasis Entity.

4.3. Each Oasis Entity that has data returned as a result of the Standard IT Searches must assign a responsible person to review the content of the data being returned in accordance with the Oasis SAR Process.

5. Overview of the Process

5.1. The SAR Manager will notify the Regional Director as well as the Data Protection Officer about the SAR, on the day of receipt, and no later than within one working day. If the SAR relates to an employment matter, the relevant PD Business Partner will act as SAR Manager and notify the Regional Director and the DPO about the SAR within the same timescales.

5.2. Upon receipt of a request, the SAR Manager should promptly respond to the requester, advising that their request is being managed and will be dealt with in accordance with applicable regulations and in line with this policy. They should advise the requester of the timelines for the return. A template acknowledgement letter is available in the separate SAR guidance notes. The Data Subject's identity should also be verified at this stage, where this is required (see section 3).

5.3. The SAR Manager will clarify the request if it is unclear (see section 6).

5.4. The DPO will advise the SAR Manager as soon as possible and may convene a telephone conference for those staff involved in responding to the SAR, where applicable. The DPO will confirm an action plan and timeline for more complex SARs.

5.5. The DPO will advise the SAR Manager on the completion of the IT search form where applicable, once the terms of the SAR are clear. The template form is in the separate SAR guidance notes. The SAR Manager will return the completed form to the IT Service Desk to request a search of Oasis's IT systems, where personal data requested are held on systems managed by the IT Services Team.

5.6. Employee requests for their personal data will involve copying the employee's personnel file. The PD Business Partner will supervise the copying of the employee's/data subject's personnel file, having first checked the file to ensure it is complete and does not mistakenly include Third party personal data. The contents will be converted to a bundle in PDF format, which is paginated, and an index will be produced in the format in the separate SAR Guidance Notes.

5.7. Employee requests for their personal data will also involve a standard download from iTrent.

5.8. In the case of data returned from IT systems other than iTrent, the IT department will de-duplicate the information as much as possible before returning it to the SAR Manager.

5.9. A decision can be taken at this point as to whether to use an external redaction company to de-duplicate the data further and/or to redact it. This is advisable where large volumes of data have been returned. See section 7.

5.10. Release of the information to the Data Subject requires the authorisation of the responsible Director for the Oasis Entity where the data subject is based.

5.11. The Director involved should ensure that the information has been reviewed prior to release to confirm that only relevant personal information relating to the Data Subject is to be returned.

5.12. Once approval has been received to release the data to the requester, the SAR Manager is responsible for preparing it in the right format. The personal data to be sent to the Requester should include a cover letter, the index to the personnel file bundle and the personnel file bundle (where there is one applicable) and the index to the OCL electronic data and the bundle of personal data from the electronic search (again, where applicable). The requested information should be arranged as far as possible in chronological order. The covering letter should include the right to lodge a complaint to the ICO and give the ICO's details. The index to the electronic data and a template response letter are both available in the separate SAR Guidance Notes.

5.13. The letter should confirm the form in which the data will be released. The data will be provided in form of PDF files, either as copies of original electronic files or as scans of original hard copy information.

5.14. Alternatively, the Information can be released through the Oasis SAR portal. The requester will be provided with a read only link to an online storage area of the SAR Portal from where they can download the information. The link will remain valid for 30 days from the point of release.

5.15. Where data is returned by post, the pack should be sent by special delivery post.

5.16. A copy of the data returned to the requester must be retained on the Oasis SAR portal to serve as a record of the data supplied.

6. Clarifying a SAR

6.1. SAR requests that are made can be general in nature and involve requests for all personal data that is processed by Oasis. However, a SAR may be for specific information and it is likely to be for the benefit of the Data Subject to provide targeted data specific to the query that they have.

6.2. The SAR Manager must seek clarification of the data requested from the Data Subject at the start of the process, without undue delay, where the information required is not clear.

6.3. The SAR Manager must not use the process of clarification to withhold information that the Data Subject may be seeking and/or to narrow the scope of the SAR unless freely requested to do so by the Data Subject. The SAR Manager should seek advice from the DPO when clarifying the requirements of a SAR with the Data Subject. The DPO can either provide specific guidance or the template form in the separate SAR Guidance Notes can be used.

7. Sifting and Redacting Information

7.1. Normally Oasis will not release information about other individuals without their explicit consent.

7.2. Once data is returned to the SAR Manager, it must be checked carefully to ensure that it does not contain Third Party personal data. If the raw information about the Data Subject also contains information related to a third party, Oasis will make reasonable efforts to anonymise that information. If this is not possible, and Oasis has been unable to secure the relevant consent, Oasis will usually be unable to release the information to the Data Subject.

7.3. Under certain circumstances, consent of other individuals will not be required prior to disclosing personal data. These circumstances include:

7.3.1. Where a member of staff is acting in their professional capacity with regards to the Data Subject.

7.3.2. Where the Data Subject would already be in possession of the information.

7.3.3. Where the information is already available in the public domain.

7.4. Third parties who regularly supply information on students/staff in a professional capacity (external examiners, referees, etc.) should be informed that anything they submit may become available to the data subject through a SAR.

7.5. Data must be sifted and redacted before it can be supplied to the Data Subject to ensure that the information released does not include information that is not relevant to the request and that it does not reveal personal or sensitive data about other Data Subjects. In addition to the above, Oasis may redact or exclude altogether some information which comes under the GDPR exemptions to SARs, listed in section 11.

7.6. Correct and compliant redaction of data is a specialist skill. Oasis will make use of a specialist third party redaction service to undertake the sifting and redaction of large volumes of data.

7.7. The costs of sifting and redaction of the data will be charged to the local budget of the Oasis Entity where the Data Subject is based.

7.8. The Oasis IT Services Team will manage the contracts with third party suppliers that are approved for use as Sifting and Redaction Service Providers.

7.9. Oasis Entities will only make use of these approved providers for Sifting and Redaction Services.

7.10 Decisions regarding exemptions or whether to redact specific pieces of information must be referred to the DPO.

8. Subject Access Requests and Children

8.1. Oasis is involved in processing a significant volume of data about children.

8.2. Oasis recognises that the child themselves is the data subject and that it is the child who holds the right of access to the data we process. Those requesting access to personal data relating to a child are able to do so if they are acting on the child's behalf regardless of their relationship to the child.

8.3. Where access is requested to personal data about a child then Oasis will always consider the best interests of the child for the information to be released including the implications of both releasing and not releasing the data.

8.4. The SAR Manager must consider if the child can understand their subject access rights. Where applicable the SAR Manager will take advice from educational professionals involved directly with the child in their consideration.

8.5. SAR Managers are advised that in most cases Oasis would consider secondary age children aged 13 or above to be able to understand their subject access rights. However, each individual data subject must be considered separately.

8.6. Where it is considered that the child is able to understand their subject access rights and where the child is aged 13 or above then positive consent is required from the child where a SAR is made on their behalf.

8.7. Where it is not considered that the child is able to understand their subject access rights then the SAR Manager must consider whether a parent or other suitable adult making the SAR is acting in the best interests of the child in deciding whether to release information to them. Where it is considered that they are not acting in the best interests of the child then the requester must be informed in writing of the decision, the reasons for the decision and the right of the requester to complain to the ICO and the ICO's details.

8.8. Any decision to release or withhold information regarding a child of primary age must be made in conjunction with the responsible Regional Director and the DPO.

9. Requests made by third parties on behalf of a data subject

9.1. A third party can make a subject access request (SAR) on behalf of a Data Subject whose data Oasis process.

9.2. The SAR Manager must be satisfied that the third party making the request is entitled to act on behalf of the Data Subject. It is the third party's responsibility to provide proof that they are entitled to make the request on behalf of the Data Subject. Oasis will not respond to Subject Access Requests made on behalf of a Data Subject by a third party where it is not completely satisfied that the third party is legitimately acting on behalf of the Data Subject. The exception to this is where the third party is the data subject's MP.

9.3. The third party making the request should supply a proof of ID from the data subject and supply ID for themselves.

9.4. SAR Managers must be mindful that changes in the scope of the SAR or the information being provided could change the ability of the third party to act on behalf of the Data Subject.

9.5. Where a SAR covers multiple Data Subjects (for example, where a solicitor makes several SARs in respect of different data subjects at the same time), then each SAR should be considered separately. Therefore, where the requester is acting on behalf of a Data Subject, information relating to the requester and information relating to the Data Subject should be considered separately.

10. Parental Access to Student Data

10.1. In Oasis, there is no automatic right for a parent to have access to personal data relating to their child via a Subject Access Request. Whilst the right for a parent to access the

educational record of a child may exist in local authority or special schools, this does not apply to Oasis academies. See section 11.2.1.

10.2. A parent is only able to make a SAR in Oasis where they are acting on behalf of their child.

10.3. Where a child is able to understand their own data protection rights and/or where the child is 13 or above (see section 8) then confirmation that a parent is acting on behalf of the child must be obtained by the SAR Manager before the information can be released.

10.4. Where a child is unable to understand their own data protection rights then the SAR Manager must consider whether providing the information to the parent would be in the best interests of the child and if they believe that the parent is legitimately acting on behalf of the child.

11. Refusals of SARs and exemptions to subject access rights

11.1. OCL can refuse a data subject's requests for data if:

11.1.1 The requests are "manifestly unfounded or excessive", "in particular because of their repetitive character" (Article 12 (5) of the GDPR) – see section 12, below.

11.1.2 We have reasonable doubt about the requester's identity and the requester has not supplied evidence of this, despite being requested to do so (Article 12 (6)).

11.1.3 The requester is not the data subject and they are not acting for them in accordance with sections 9 and 10.

11.1.4 The data requested fall within the exemptions below.

11.1.5 It is mixed data, where disclosure would adversely affect the rights and freedoms of others, and the problem cannot be remedied by redaction or the other solutions in this policy – Article 15(4).

11.2 Exemptions to the rights of access are as follows:

11.2.1 Educational records – As we are an Academy sponsor, students' educational records are exempt from disclosure under Schedule 3, part 4 and paragraph 14(1) & 14(3)(b) of the Data Protection Act (DPA) 2018.

11.2.2 SEN Records – Any information relating to SEN is exempt information under the DPA 2018. This is because Schedule 4, section 4 of the DPA 2018 exempts students' statements of special educational needs from disclosure under a subject access request.

11.2.3 Child Abuse Data – Schedule 3, Part 5 and paragraph 21 of the DPA 2018 excludes requests for child abuse data from the subject access provisions under Article 15(1) to (3) of GDPR, to the extent that releasing that data would not be in the best interests of the data subject

11.2.4 Legal Professional Privilege – this covers confidential communications between Oasis and our professional legal advisers where litigation is contemplated or in progress – DPA 2018, Schedule 2, Part 4, paragraph 19.

11.2.5 References – given by Oasis in confidence and for the purposes of an individual's education, training or employment or the provision of a service by them. However, this exemption to subject access rights does not apply to any references Oasis has received. – DPA 2018, Schedule 2, Part 4, paragraph 24.

11.2.6 Management forecasts – personal data that is processed for management forecasting or planning purposes – DPA 2018, Schedule 2, Part 4, paragraph 22.

11.2.7 Negotiations with the requester – personal data that consists of a record of Oasis's intentions in negotiations with an individual is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice these negotiations – DPA 2018, Schedule 2, Part 4, paragraph 23.

11.2.8 Exam scripts or exam marks – DPA 2018, Schedule 2, Part 4, paragraph 25.

11.3 Advice should be sought from the DPO in the event that Oasis wishes to apply any of these exemptions. The DPO should document the advice given and notify the Oasis Audit and Risk Committee of the Board.

12. Excessive or disproportionate SARs

12.1. Right of subject access is fundamental to data protection. DPA places high expectation on Oasis to make extensive efforts and provide requested information to a Subject Access Request (SAR). However, searches in response to general requests for information can return significant volumes of data, which can in turn place a significant burden on the organisation to be able to effectively sift and redact the content to ensure the data protection rights of other data subjects are not adversely impacted by the release of information.

12.2. It is Oasis policy to store personal and sensitive information in dedicated systems and within filing systems which will make its retrieval and preparation in response to a SAR straightforward and rapid. Information stored in these locations should be provided (in a suitably sifted and redacted form) as a matter of course.

12.3. Where the scope of the SAR is found to place an excessive administrative burden on the organisation then the SAR Manager must seek clarification as to the information that is required whilst remaining mindful of 6.3 in this policy.

12.4. Where clarification of the scope of the SAR does not reduce the level of administrative effort to a manageable amount then the SAR may be considered excessive and may be declined (see section 12.7), although reasonable efforts will always be made to fulfil the SAR.

12.5. Oasis will not limit the number of SARs an individual can make. However, Oasis will only comply with identical or similar SARs from the Data Subject if a period of more than 12 months has lapsed.

12.6. SARs covering different time periods are not considered to be similar or identical.

12.7. The SAR Manager must obtain permission from the DPO and the Chief Operating Officer before declining a SAR due to the excessive nature of the request. The DPO should document the advice given and notify the Oasis Audit and Risk Committee of the Board.

12.8. Where a SAR is declined due to its excessive nature, the SAR Manager must write to the Data Subject, making clear the reasons for the SAR being declined and advising the Data Subject of their right to complain to the Information Commissioners Office (ICO).

13. Subject Access Requests and Freedom of Information Requests

13.1. Any FOI request must be forwarded on as soon as possible to be separately addressed under OCL's Freedom of Information Policy.

13.2. A valid SAR may be received in the form of or described incorrectly as a Freedom of Information (FOI) request. This may be either due to an incorrect understanding of FOI regulations on the part of the Data Subject or due to both an FOI and SAR being combined.

13.3. Oasis will respond to SARs received in the form of or described as FOI requests where they are valid.

13.4. Information requested as a SAR may be available to the requester under FOI. Where this is received then the FOI request and any SAR must be managed separately.

13.5. The SAR Manager will write to the requester as soon as is possible after the request is received and explain where the response is being dealt with as a SAR and where it is being dealt with as an FOI request.

14. Subject Access Requests for CCTV

14.1. Data Subjects have the right to request access to CCTV footage relating to themselves without infringing on the rights and freedoms of third parties.

14.2. Data Subjects who request access must provide clarification details that allow us to identify them as the subject of the information and to locate the information. For example, date, time and location.

14.3. Access may be provided by allowing the Data Subject to view the footage rather than in the form of a copy of the personal data where appropriate.

14.4. In responding to a SAR, consideration will be given to obscuring identifying feature of any other individuals in the image. Where there are no grounds for disclosing the personal data of another data subject (see section 7) or where Oasis is unable to release the information for other reasons (see section 11) Oasis reserves the right to refuse access to CCTV footage.

15. Timelines

15.1. Normally, Oasis will respond to a SAR within 30 calendar days.

15.2. Where Oasis needs more time to respond (due to volume or complexity), the SAR Manager must inform the requester with an explanation for the delay as soon as possible, and in any event within 30 calendar days.

15.3. Extensions can only be requested with the authorisation of the DPO.

15.4. The maximum time that Oasis may request for a SAR is 90 days.

15.5. Oasis may ask the requester for additional information to help locate the data relating to the SAR. The SAR Manager should respond promptly to a SAR unless we reasonably require more details to help find the requested data.

15.6. The timeline for the SAR will start at the point it is received except where there are some specific circumstances involved:

15.6.1. Where a request is received through the post this will be assumed to be the post mark plus 2 days; unless the letter was signed for where the date of the signature will be used or where information was held externally by a third party such as the Royal Mail holding post during the holiday periods. Where this is the case then the start date will be considered to be the date when deliveries were resumed. Where the mail is received but the Oasis Entity is not open, then the postmark date will apply.

15.6.2. Where clarification is required in order to be able to locate the information requested then the time line starts from the point at which the response to the clarification is received.

16. Deleted information and information stored in IT backups

16.1. Oasis will not search for and recover deleted information from IT Backups and provide it to a data subject in response to a SAR unless there is a request for some specific information which is only held in backup.

16.2. Where access to data is required that is not available in a live system, the specific information regarding the location of the data and the time when it was present will be required from the Data Subject.

17. Charging

17.1. The information must be provided free of charge.

18. Training

18.1. All staff are trained to recognise a SAR as part of the general data protection training. More detailed training on handling SARs is provided to relevant staff, dependent on job role.

19. Monitoring compliance

19.1. Compliance with SARs and with this policy is monitored and discussed at senior management and Board level. Management information is kept by the DPO showing the number of SARs received and their details, to verify compliance.

Appendix 1 – RACI Matrix

R = Responsible A = Accountable C = Consulted I = Informed

Policy Element				Leadership					Academy				Services				IT Team							
	Requestor	Policy Owner	SAR Manager	Group CEO	OCL CEO	OCL COO	National Director	Regional Director	Academy Principal	Designated Representative	Teacher	Academy User	Head of National Service	Data Protection Officer	PD Regional Business Partner	National Service User	Director of IT Services	Head of IT Service Delivery	National Infrastructure Manager	Service Desk Manager	National Service Desk	Service Delivery Manager	Cluster Manager	Onsite Teams
1.1-1.2 Openness and Transparency				A	R	R	R	R	R	R			R	R	R		R							
1.4 – 1.6 Form of SAR				A	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
1.7 – 1.10 Clarification of the SAR	A								C	C				C	C				I	I	I			
2.1 Accountability for a SAR (Academy Student)					I	I		C	A	C				C										
2.1 Accountability for a SAR (Academy Staff Member)					I	I		A	C	C				C	C									
2.1 Accountability for a SAR (National Staff Member)					I	A							C	C	C									
2.2-2.3 Assigning the SAR Manager (Academy Student)								C	A															
2.2-2.3 Assigning the SAR Manager (Academy Staff Member)								A	C					C	C									
2.22.3 Assigning the SAR Manager (National Staff Member)						A								C	C									
2.4 Informing the DPO (Academy Staff / Student)			R						A															
2.4 Informing the DPO (National Staff)			R												A									
2.5 Maintaining a Register of SARs														A										
2.6 Keeping the DPO Informed			A						R						R									
2.7 Management of the SAR			A																					
2.8 Providing Advice / Support														A	R		C	C	R		R	C		

2.9 Management of wider context (Academy)									A					C	C									
2.9 Management of wider context (National Staff)													A	C	C									
3.1, 3.3-3.5 Identifying the Requestor			A						R				R	C	C									
3.2 Providing Sufficient Information to verify identity	A																							
4.1 – 4.3 Cross Oasis Entity SARs			A			C								C			C	C	C					
5.1 (Process) Notification of the SAR			A												C									
5.2 (Process) Communication with the Requestor			A											C	C									
5.3 (Process) Seeking Clarification			A											C	C									
5.4 (Process) Development of Action Plan			C					C	C	C			C	A	C		C	C	C	C		C		
5.5 (Process) Completion SAR IT Search Form			A											C	C		C	C	C	C		C		
5.6 (Process) Staff Personnel File			R											C	A									
5.7 (Process) Staff iTrent Report			R											C	A									
5.8 (Process) De-Duplication of IT Data			I											I	I				A	R	R			
5.9 (Process) Decision on Redaction Mechanism			I			C		C	I	I				A	C		C		I	I	I			
5.10 - 5.11 (Process) Release of Information to Data Subject			R					A	C	C				C	C									
5.12 – 5.16 (Process) Preparation of Return (Academy)			A					C	C	C				C	C									
5.12 – 5.16 (Process) Preparation of Return (National Staff)			A			C							C	C	C									
6.1 – 6.3 Clarification			A											C	C									
7.1 – 7.3 Sifting and Redaction			A											C	C									
7.4 Informing Professional Third Parties									A	R				C										
7.5 Sifting and Redaction			C											A	C									
7.6 - 7.9 3rd Party Sifting and Redaction Services			I					C	I	I				C	C		A	R	R	R		R		
7.10 Exemption Decisions						C		C	C					A	C									
8.1-8.8 Release of Children's Data			R					A	C	C				C	C									
9.1 – 9.5 SARs by Third Parties			R					A						C	C									
10.1 – 10.4 Parental SAR Rights			R					A						C										
11.1 – 11.3 Refusal of a SAR			R			A		C	C				C	C	C									
12.3 – Clarification of the SAR			A																					
12.4 – 12.7 Declining a SAR as Excessive			R			A		C	C				C	C	C									

12.8 Informing the Data Subject			A			C		C	C	I			C	C	C									
13.1 - 13.5 SARS and FOIs			A			C			C	C			C	C	C									
14.2 Clarification of CCTV Footage access			A			I			C	C			C	C	C									
14.3-14.4 Providing Access to CCTV			A																					
15.1 Responding to a SAR with 30 Days			A			C		C	R	R				C	R									
15.2 Informing the Data Subject of Timeframe			A																					
15.3 – 15.4 Authorisation of Extensions			C			C		C	C				C	A	C									
16.1 Providing Information from Backups																	A	R	R	R	R			
16.2 Clarification of information required from Backups	A		R																					
17.1 Providing SAR Returns Free of Charge			R	A	R	R	R	R	R	R			R	R	R									
18.1 Staff Undertake SAR Training				A	R	R	R	R	R	R			R	R	R									

Document Control

Changes History

Version	Date	Owned and Amended by	Recipients	Purpose
V0.1 – 0.6	Oct 2017	Amended by Shalin Chanchani	Rob Lamont, Steve Hobbs	Initial drafts
V0.7- 0.9	June 2018	Amended by Sarah Otto	OCL	DPO review
V1.0	June 2018	Amended by Sarah Otto	OCL	DPO review
V1.1	Jan 2019	Amended by Rob Lamont	Sarah Graham, Sarah Otto	Updated
V2.0	April 2019	Amended by Sarah Graham	Rob Lamont, Sarah Otto	Updated
V2.2	April 2019	Amended by Rob Lamont	For Consultation	RACI Added
V2.21	May 2019	Amended by Rob Lamont	Updated following feedback from ICO	For Review by CSG

Policy Tier

☒ Tier 1

☐ Tier 2

☐ Tier 3

☐ Tier 4

Owner

Rob Lamont

Contact in case of query

Sarah.otto@oasisuk.org

Approvals

This document requires the following approvals.

Name	Position	Date Approved	Version
CSG	CSG	20th May 2019	2.21

Position with the Unions

Does the policy or changes to the policy require consultation with the National Unions under our recognition agreement?

☐ Yes

☒ No

If yes, the policy status is:

☐ Consulted with Unions and Approved

☐ Fully consulted (completed) but not agreed with Unions but Approved by OCL

☐ Currently under Consultation with Unions

☐ Awaiting Consultation with Unions

Date & Record of Next Union Review

Location

Tick all that apply:

☒ OCL website

☒ Academy website

☒ Policy portal

☐ Other: state

Customisation

☒ OCL policy

☐ OCL policy with an attachment for each academy to complete regarding local arrangements

☐ Academy policy

☒ Policy is included in Principals' annual compliance declaration

Distribution

This document has been distributed to:

Version	Date	Owned and Amended by	Recipients